ESRI
EXTERNAL

April 2020

Discovering and Limiting Access to Public Survey123 Results

Version 1.7

Esri Software Security and Privacy

380 New York Street
Redlands, California 92373-8100 USA
909 793 2853
info@esri.com
esri.com

esri THE SCIENCE OF WHERE®

Copyright © 2020 Esri
All rights reserved.
Printed in the United States of America.

The information contained in this document is the exclusive property of Esri. This work is protected under United States copyright law and other international copyright treaties and conventions. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, except as expressly permitted in writing by Esri. All requests should be sent to Attention: Contracts and Legal Services Manager, Esri, 380 New York Street, Redlands, CA 92373-8100 USA.

The information contained in this document is subject to change without notice.

Esri, the Esri globe logo, The Science of Where, ArcGIS, esri.com, and @esri.com are trademarks, service marks, or registered marks of Esri in the United States, the European Community, or certain other jurisdictions. Other companies and products or services mentioned herein may be trademarks, service marks, or registered marks of their respective mark owners.

Abstract:

Designing and configuring a Survey with an underlying survey layer can be tricky when the survey is intended to be completed by the public. Discovering insecure survey layers can be challenging for an organization administrator responsible for ensuring collected data is secure and configured to respect respondent privacy. This document provides guidance for GIS administrators, survey owners or users involved in implementing a public survey with respect to privacy and security. The following guidance highlights best practices, public survey layer discoverability, details specific scenarios, and provides contextual discussion around the various configuration options to be considered to protect your data prior to announcing a public survey where results are to remain secure.

Public Surveys

What is a survey?

Surveys created by Survey123 are designed to enable rapid collection with predefined questions that use logic and provide easy-to-fill answers, embedded audio and images, and offer many languages. Surveys consist of survey forms and survey layers. In Survey123 a survey form is fillable form containing questions and lists of potential static or free form responses. Responses to questions asked in surveys are collected in survey layers.

What is a survey layer?

A survey layer is a feature service hosted on ArcGIS Online or ArcGIS Enterprise which contain the database schema and records and other objects collected from users completing the survey form.

What do we mean by a ‘public survey’?

By definition, a public survey is accessible to anyone who wants to submit data to it, but that does not always mean that anyone should be able to look at the data that has been submitted. A frequent use case is anonymously collecting survey data. Depending on the use case, it may be desirable that only a select few administrators or survey owners should be allowed to review the responses. In other cases, the intent of the survey may be to immediately publish the data collected. This guide seeks to provide guidance for the former scenario.

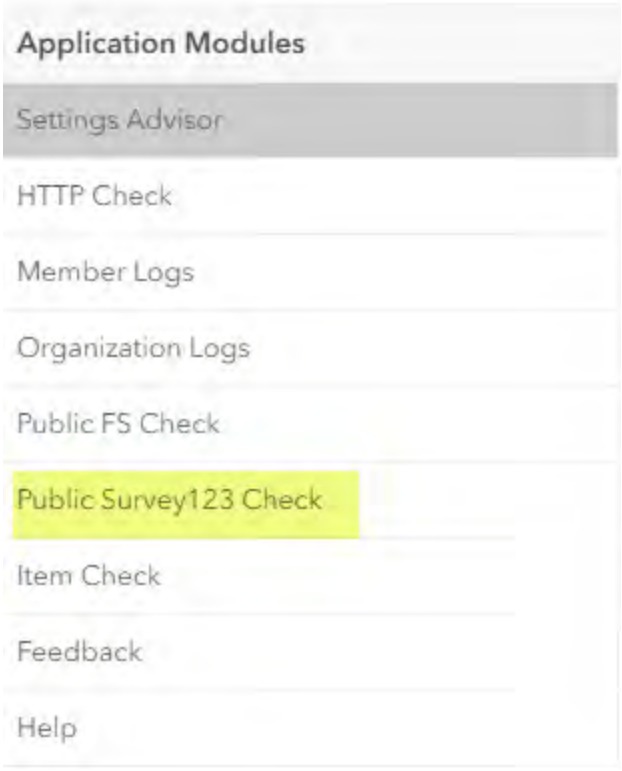
How might data be compromised in public surveys?

Improperly configured public surveys containing survey layers with the 'update' and 'query' capabilities enabled can allow unauthorized individuals to change, delete, export, or add incorrect or misleading data to your survey layers via the ArcGIS Rest API. These activities may have significant impacts to data security, with impacts to data confidentiality and to the assurance that the origin, authenticity, and integrity of the data can be properly verified.

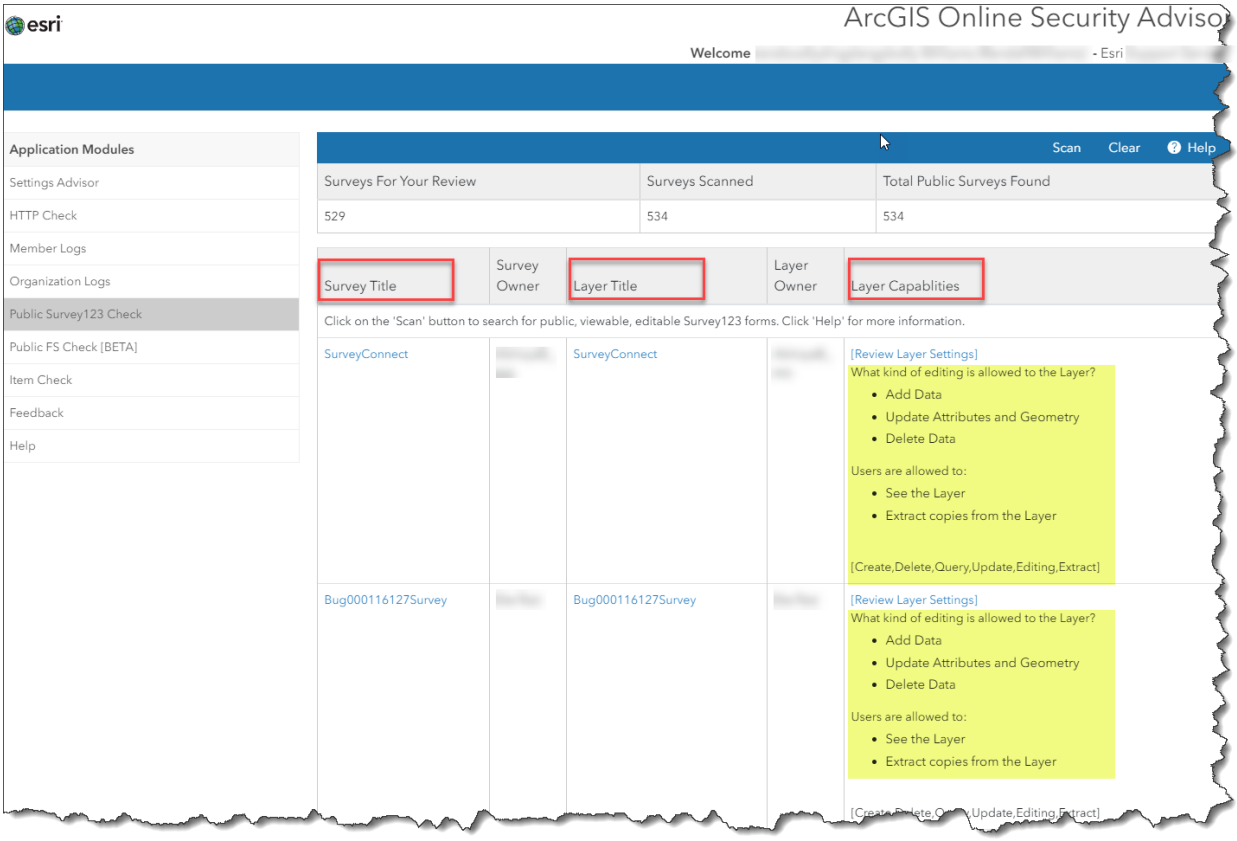
Discovering public survey layers

For large ArcGIS Online or ArcGIS Enterprise customers with many users and substantial content, it can be time consuming to navigate through all the survey forms and layers hosted in organization to validate each item's sharing and editor settings. The Esri Software Security and Privacy Team has developed a "Public Survey123 Check" tool for the ArcGIS Online Security Advisor. The ArcGIS Security Advisor's purpose is to provide customers with security awareness regarding their ArcGIS Online organization's configuration settings and content. The ArcGIS Online Security Advisor is managed and supported by the Esri Software Security and Privacy team.

To access the Public Survey123 Check tool, first navigate to the ArcGIS Online Security Advisor and click the Sign-In button. Sign in using a member of your ArcGIS Online organization with administrator role privileges and select the Public Survey123 Check module.



The Public Survey123 Check module allows an ArcGIS Online Organization administrator to quickly query and discover information about public survey forms and their associated survey layers. It allows administrators to understand the number of public surveys that are active in the organization, lists titles for both publicly shared surveys and their associated survey layers, documents the survey layer's owner, and describes the edit capabilities that are currently enabled for the survey layers. Administrators may click the "Go to settings" link to open the survey layer's settings in the ArcGIS Online home application and update the editing options as needed.



Suggested editing options are provided in the topic "Controlling permissions in the survey layer from your ArcGIS Online Organization or your ArcGIS Enterprise Instance", covered later in this paper.

Securing data in public surveys

Data security is a very important factor when configuring surveys that might collect sensitive information. If your public Survey123 form contains sensitive information, you will need to configure your survey layer(s) to prevent users in the public domain from downloading, querying or changing data that has submitted. Securely configuring your survey layers helps to ensure the confidentiality and integrity of the information that has been collected.

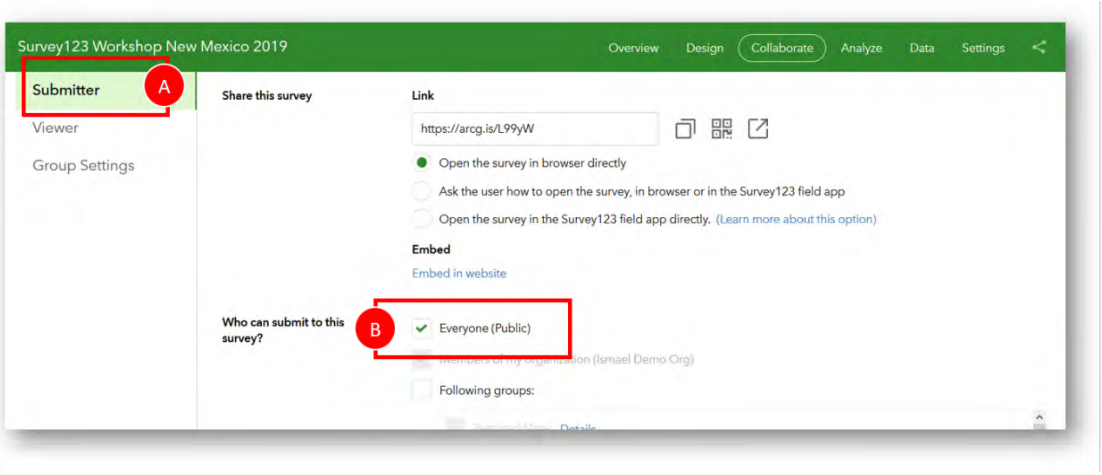
Unfortunately, it is not uncommon to find public surveys where the security configuration of the survey layer is not appropriately configured, allowing unauthorized access to the survey's data. Configuring proper access controls for survey layers can help prevent embarrassing and costly data exposure, potentially placing your organization at legal risk. Consider the following options and workflows when configuring your public survey layers to limit the exposure of sensitive data.

Sharing your survey with the public from the Survey123 website

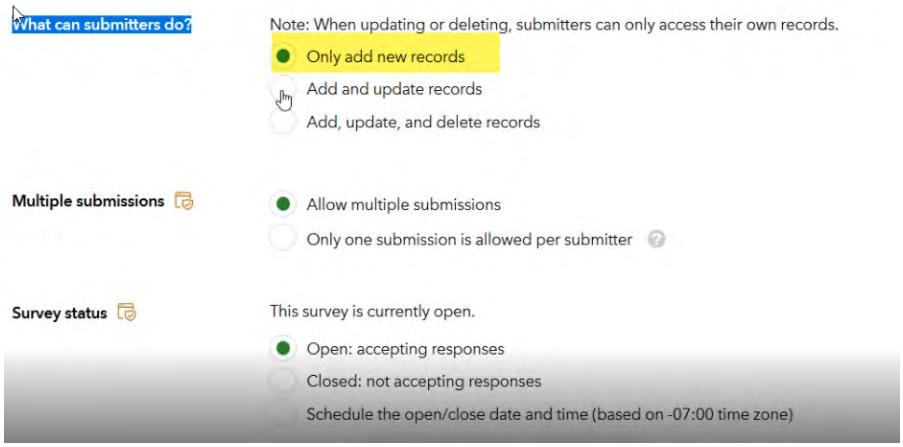
First, a survey owner will need to share the survey form to the public to allow the audience to submit information without providing authorization credentials. To do this, the survey manger will need to access the Survey123 website at https://survey123.arcgis.com.

1. To ensure that your survey is shared with the public, log into the Survey123 website, and open the Collaborate tab of your survey.

    a. From the Collaborate tab, ensure the Submitter section is selected (A), and then
    b. Check the Everyone' checkbox (B) next to the 'Who can submit to this survey?' option.



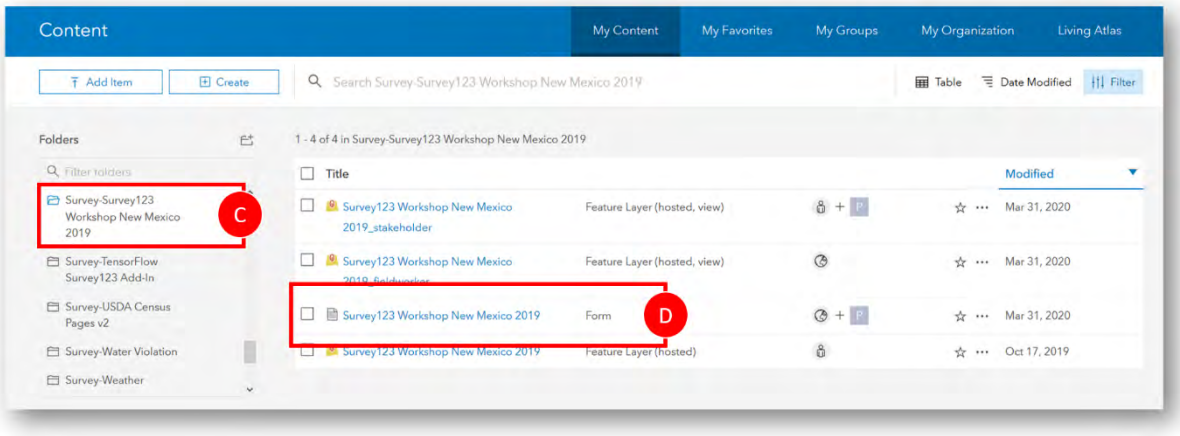
    c. Review the additional options for what submitters can do with the survey. Surveys where sensitive information is collected should be configured to allow submitters to only add new records. Add and update or add, update, and delete records should be **disallowed (unchecked)**, because these options allow users to query the survey layer and potentially export or modify data.



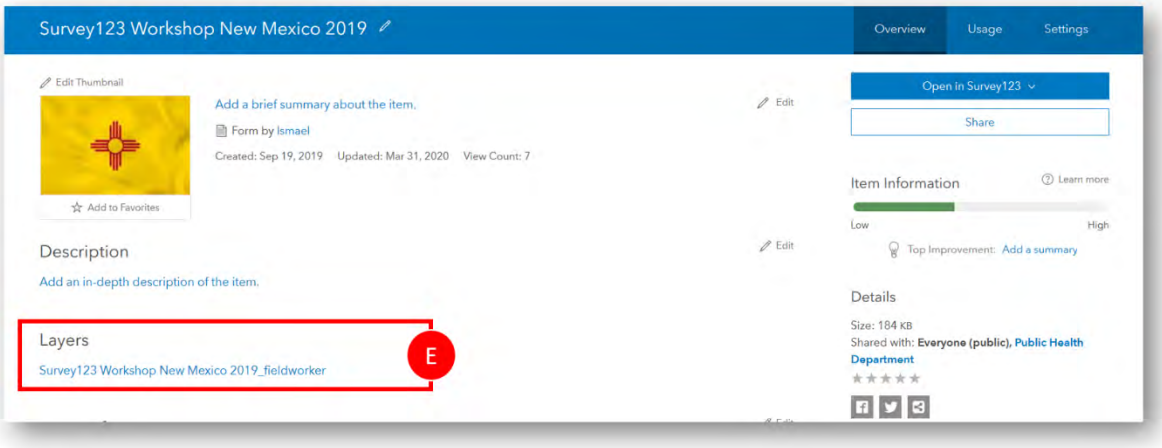
Controlling permissions in the survey layer from your ArcGIS Online Organization or your ArcGIS Enterprise Instance

Next, you'll need to configure the security options for the underlying survey layers that support the survey. These options will be set in the survey layer's properties in the item detail page in either the ArcGIS Online Organization or the ArcGIS Enterprise instance. To configure these options, either click the "Go to settings" link in the Survey123 Check module in the ArcGIS Online Security Advisor or use the ArcGIS Online Home app to navigate to the survey layer settings. If you are accessing survey layer edit settings by using the "Go to settings" module in the ArcGIS Online Security Advisor, skip to step 'e'.

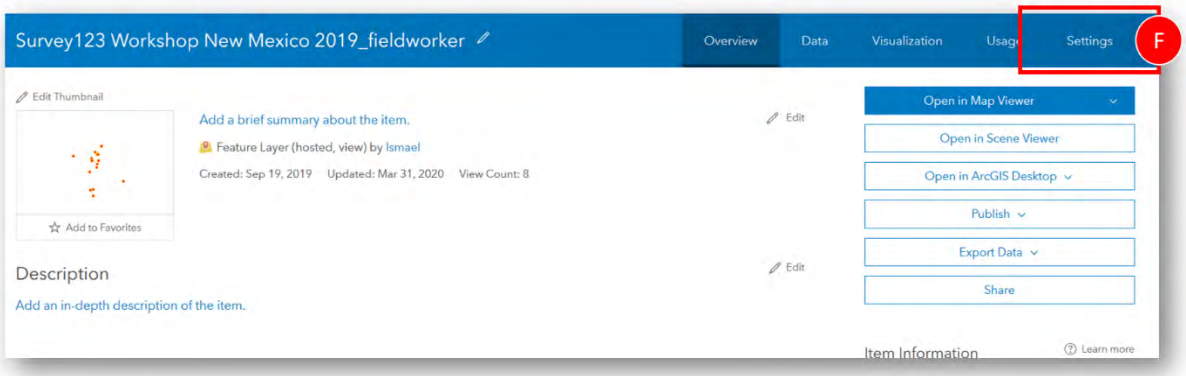
a. Log into ArcGIS.com or your ArcGIS Enterprise portal and navigate to the Content tab.
b. Open your survey's folder. Note that your survey's folder name will have a Survey13- prefix followed by the name of your survey. (C) Click on the Form item within your folder to access the item details page of your Form item (D).



c. Next, in the Form item details page, click on the Layer name (under the Layers heading) to open the details page of your survey layer (E).



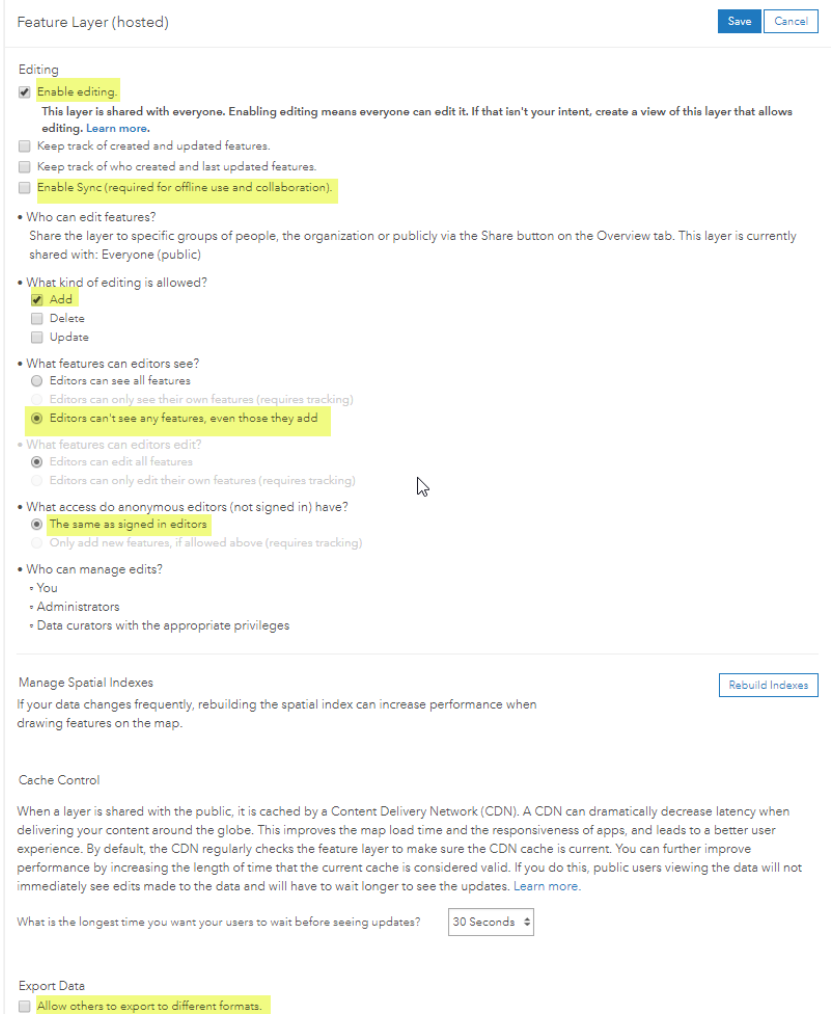
d. In the details page of your survey layer, click the Settings tab (F) and scroll to the bottom.



e. The Layer Settings tab exposes fine grained controls over permissions for your survey layer. Review these options carefully. Refer to the "editor settings" documentation for a full description of the various settings available. To ensure that the data that you've collected is not exposed to others, select the following options and refer to the exhibit below:

Option	Value
Enable editing	Checked
Enable sync	Not Checked
What kind of editing is allowed?	"Add"
What features can editors see?	"Editors can't see any features, even those they add."
What access do anonymous editors (not signed in) have?	"The same as signed in editors"
Allow others to export to different formats?	Not checked

Exhibit: Survey Layer Editor Settings



f. In the upper right corner, click to SAVE your changes to the survey layer to persist your changes and to ensure that the data that you've collected will not be exposed through your survey or the underlying survey layers.

Feature Layer views

The ability to create a feature layer view is a powerful feature in ArcGIS Online and ArcGIS Enterprise. Hosted feature layer views allow you create multiple unique windows into your data and customize them to fit your audience. Views you create reference the same primary feature layer so there is no duplication of data. Hosted feature service views can be used to allow survey owners to anonymize results, change symbols, and otherwise display data in different ways depending on the audience and use case.

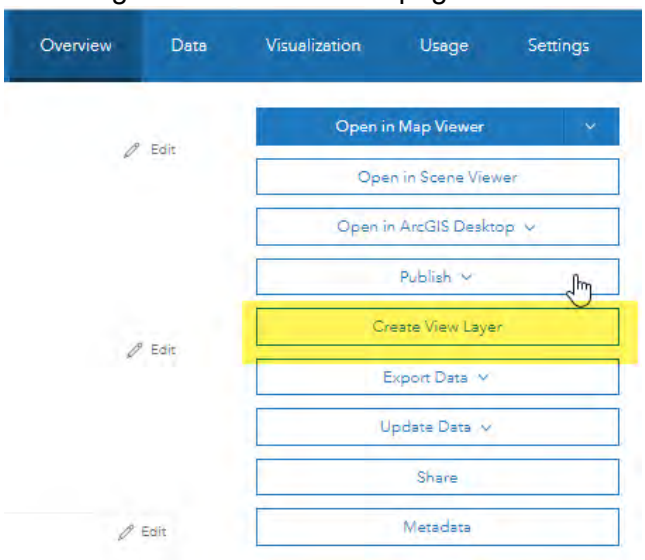
Hosted feature layer views are ideal for helping you control access to the hosted feature data; you can allow editing access to only those users who need it. You can make your hosted feature layer editable and share it with only those groups whose members need to edit the data.

Then you can create hosted feature layer views from the hosted feature layer, don't enable editing on them, and share the views to audiences with appropriate access to the data you've collected.

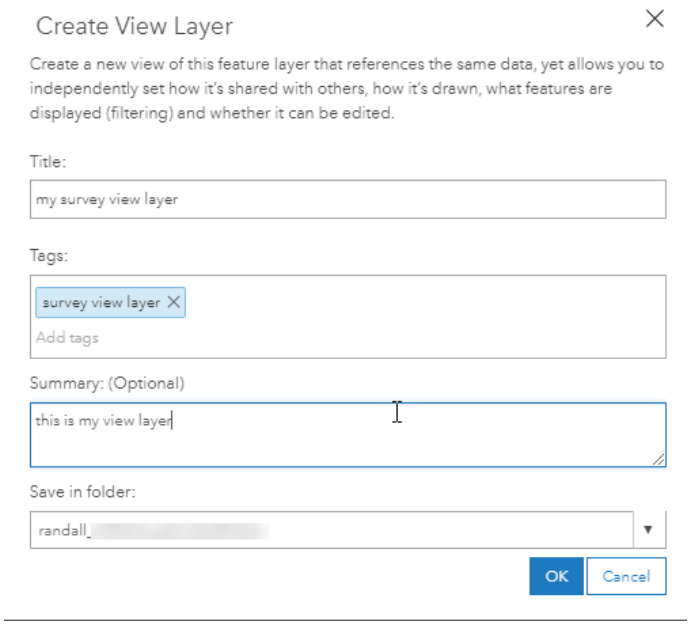
Using Feature Layer views to summarize results

After completing the steps to configure your survey and survey layers, you may choose to create a new view layer. The view layer may be referenced in a dashboard, web map, or other application for review. To create a feature layer view, first access the item details page of your survey layer, just like you did in step "b" above.

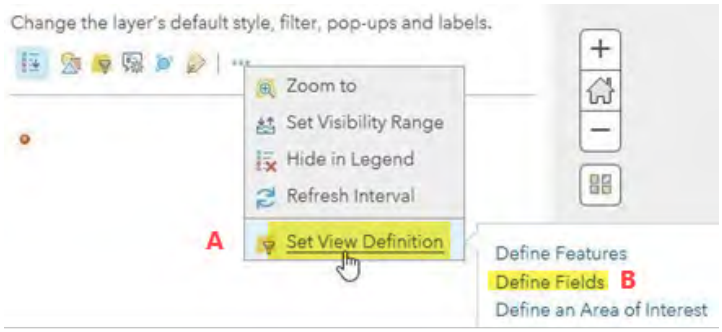
g. To the right of the item details page in the "overview" tab, click "Create a View Layer"



h. Provide a title and metadata for the view layer and click "ok"



i. Open the “Visualization tab.
j. Click the ellipsis, then select “Set View Definition” (A),
k. then “Define Fields” (B)



l. Check the boxes next to the fields that should be available in the view layer. Make sure to only check the option to display fields users that the audience of this view layer should access.

m. Explore the other options in the Visualization tab to aggregate features, create heat maps, and further anonymize data to reduce or eliminate any personally identifying information as your mission requires. Using the Visualization tab, you can make changes to the default properties of a feature layer without having to open the layer in Map Viewer. You can change the layer’s style, apply a filter, configure pop-ups, or label the features in the layer. You can also hide the layer in the legend or change the refresh interval. As in Map Viewer, the Visualization tab provides navigation tools to explore the layer, access to the basemap gallery, and a search box to find an address or place.

n. Finally, add the view layer to a new web map to be consumed by a dashboard, application, or other WebGIS client.

Summary: Securing data in public surveys

To guarantee that your sharing and permissions are consistent and set to your preferences, it is highly recommended that you always use the Collaborate tab in the Survey123 website to define who can submit data to your survey, and then the editor permissions in ArcGIS Online (or ArcGIS Enterprise Portal) website to define the specific permissions granted in your survey layer.

If you want to enable access to your survey data for use within your organization, or want to share publicly certain data (rows or fields) of your survey data, it is strongly recommended you create new Feature Layer views on top of your survey layer and control permissions and access separately for that purpose.

The advice and steps provided in this document will prevent your public survey from exposing your survey data for public access while allowing anyone to submit data through your form.

esri | THE SCIENCE OF WHERE®

Esri, the global market leader in geographic information system (GIS) software, offers the most powerful mapping and spatial analytics technology available.

Since 1969, Esri has helped customers unlock the full potential of data to improve operational and business results. Today, Esri software is deployed in more than 350,000 organizations including the world's largest cities, most national governments, 75 percent of Fortune 500 companies, and more than 7,000 colleges and universities. Esri engineers the most advanced solutions for digital transformation, the Internet of Things (IoT), and location analytics to inform the most authoritative maps in the world.

Visit us at esri.com.

Contact Esri

380 New York Street
Redlands, California 92373-8100 USA

1 800 447 9778
T 909 793 2853
F 909 793 5953
info@esri.com
esri.com

Offices worldwide
esri.com/locations

For more information, visit **https://trust.arcgis.com**.